Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

COMMENTS OF VERIZON

Michael E. Glover
Of Counsel

Karen Zacharia
Joshua E. Swift
VERIZON
1515 N. Court House Road
Suite 500
Arlington, VA 22201-2909

Scott Delacourt
Wiley, Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006

Counsel for Verizon

Dated: April 28, 2006

EXECUTIVE SUMMARY

Verizon is committed to protecting its customers' privacy and has implemented comprehensive measures to protect customer information. To this end, the company reviews and modifies its data security measures on a regular basis to minimize the possibility of improper disclosure of customer information while at the same time providing quality service to its customers.

As it considers changes to the CPNI rules in response to the EPIC Petition, the Commission should be flexible and balanced in its approach. Flexibility is critical to addressing the threat posed by data brokers who constantly alter their tactics. Any new tools developed by the Commission to address the security of confidential customer information should afford carriers the flexibility they need to respond to this threat. At the same time, the Commission must balance the need to protect customer data against other important business considerations. It should be careful to avoid imposing unnecessary burdens on customers who have legitimate needs for accessing account information. In addition, it should be mindful of the costs imposed by new regulations – including re-engineering systems and re-training employees – and avoid expensive, burdensome measures which increase the cost of service to customers while offering little or no data security benefit.

Consistent with these principles, there are a number of practices the Commission should encourage by making them the basis for "safe harbor" protection from enforcement action. Specifically, Verizon supports a "safe harbor" incorporating the following practices:

(1) carrier cooperation with FCC, FTC, and DOJ efforts to identify and prosecute data brokers;

(2) participation in a carrier working group dedicated to enhancing data security and combating theft of confidential information;

(3) permitting customers to voluntarily elect password protection for residential accounts;

(4) filing of more detailed annual CPNI certifications with the FCC;

(5) posting privacy policies online; and

(6) establishing certain categories of information – such as social security, driver's license, and taxpayer identification numbers – that should not be disclosed to residential customers.

Carriers adopting these practices should receive "safe harbor" protection from enforcement action, consistent with the Commission's approach in the do-not-call context.

Certain other measures proposed in the *Notice*, however, should be rejected as unduly burdensome in light of their limited benefit. The Commission previously rejected an audit trail requirement as unduly burdensome, and it should not revisit that decision here. Other proposed measures would impose burden and expense without addressing the data broker threat. Encryption, for example, is principally a defense against hacking, while it appears that data brokers proceed chiefly by pretexting – that is, through guile, deception, and impersonation. Similarly, while the purpose of data retention regimes is to protect older and archived data, there is no evidence that such information has been a target of data brokers. In addition, some proposed measures could undermine data security or confuse customers. For example, customer notification of possible security breaches might lead customers to ignore CPNI notices entirely or needlessly worry about disclosures that have not occurred. Likewise, a customer option to impose an "absolute" no release order on an account might impede legitimate transactions without increasing security. In addition, the Commission should not adopt any new measures for business customers. Many business customers have contractual or other specialized security

arrangements with their local service providers and, in any event, business customers have not been the target of data brokers.

Finally, the Commission should reject calls to revisit settled law with respect to opt-in/opt-out consent. The opt-out rules do not have any connection to the data broker problem. Moreover, the proffered alternative – an opt-in regime – is unconstitutional and unwise as a matter of policy.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

COMMENTS OF VERIZON[1]

Verizon is committed to protecting its customers' privacy and has implemented comprehensive measures to protect customer information.[2] To this end, the company reviews and modifies its data security measures on a regular basis to minimize the possibility of improper disclosure of customer information while at the same time providing quality service to its customers.

As it considers changes to the CPNI rules in response to the EPIC Petition,[3] Verizon urges the Commission to be flexible and balanced in its approach. Flexibility is critical to

---

[1] The Verizon companies participating in this filing ("Verizon") are the regulated, wholly owned subsidiaries of Verizon Communications Inc.

[2] *See, e.g.*, Verizon, *Privacy and Customer Security Policies* (Jan. 2005), *available at* http://www22.verizon.com/about/privacy/customer/; Verizon Wireless Privacy Statement, *available at* http://www.verizonwireless.com/b2c/footer/privacy.jsp.

[3] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, RM-11277 (filed Aug. 30, 2005) ("EPIC Petition").

addressing the threat posed by data brokers who constantly alter their tactics.[4] Any new tools developed by the Commission to address the security of confidential customer information should afford carriers the flexibility they need to respond to this threat. At the same time, the Commission must balance the need to protect customer data against other important business considerations. It should be careful to avoid imposing unnecessary burdens on customers who have legitimate needs for accessing account information. In addition, it should be mindful of the costs imposed by new protections – including re-engineering systems and re-training employees – and avoid expensive, burdensome measures which increase the cost of service to customers while offering little or no data security benefit. This is a particular concern with respect to transactions – such as ordering new services – that do not involve CPNI. Finally, the Commission should not impose new regulations on carriers and classes of customers, such as business customers, where there is no evidence that they are needed.

I. THE COMMISSION SHOULD SUPPORT CARRIERS IN COMBATING DATA BROKERS AND ENCOURAGE PRACTICES THAT ENHANCE CUSTOMER DATA SECURITY WHILE PRESERVING CARRIER FLEXIBILITY.

The Commission should establish a "safe harbor" in which carriers are not liable for a penetration of their systems if they have adopted appropriate data protection practices, similar to the "safe harbor" provision in the Commission's do-not-call rules.[5] There are a number of specific "safe harbor" practices the Commission should encourage to enhance security of residential customer data, including working with the Federal Trade Commission ("FTC"), Department of Justice ("DOJ"), and the industry to bring data brokers to justice. It should encourage carriers to: (1) post privacy policies online; (2) provide residential customers with the

---

[4] Verizon uses the term "data brokers" to refer to persons who claim to be able to provide customer proprietary network information ("CPNI") to others for a fee. *See* EPIC Petition at 1-2.

[5] 47 C.F.R. § 64.1200(c)(2).

option of password protection on a customer account; and (3) never disclose to callers certain categories of particularly sensitive information (such as social security numbers). The Commission also should support carrier efforts to make reasonable revisions to their annual CPNI certifications, so that the Commission can better track carriers' efforts to address the data broker problem. Affording "safe harbor" protection will encourage carriers to adopt these practices while recognizing that, due to the nature of the data broker threat, some wrongdoers may still achieve unauthorized access to customer data despite carrier diligence.

A. The Commission Should Work With Carriers, The Federal Trade Commission, And The Department Of Justice To Identify And Prosecute Data Brokers.

As an initial matter, the best way to attack the problem is to go after its source: the wrongdoers themselves. Verizon Wireless, EPIC, and others have brought actions in the courts and before the FTC to stop some of the more egregious violators.[6] The Commission should work with the FTC and the DOJ to develop methods for bringing these parties to justice. For example, the agencies could create a hotline or website link to report suspected illegal activity and create a joint task force to examine the best ways to shut down such operations.[7] Industry

---

[6] *See, e.g.*, News Release, Verizon Wireless, *Theft of Verizon Wireless Customer Records by Tennessee Company Halted* (Sept. 15, 2005), *available at* http://news.vzw.com/news/2005/09/pr2005-09-15.html; Electronic Privacy Information Center's Complaint and Request for Injunction, Investigation and for Other Relief, *In re Intelligent e-Commerce, Inc.* (Fed. Trade Comm'n July 7, 2005), *available at* http://www.epic.org/privacy/iei/ftccomplaint.html; *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003); *FTC v. Information Search Inc.*, Stipulated Final Judgment and Order, No. AMD01-1121 (D. Md. Mar. 15, 2002), *available at* http://www.ftc.gov/os/2002/03/infosearchstip.pdf; *FTC v. World Media Brokers Inc.*, Memorandum Opinion and Order, No. 02-CV-6985 (N.D. Ill. Mar. 1, 2002), *available at* http://www.ilnd.uscourts.gov/racer2.

[7] The Commission and the FTC have worked together on several initiatives in the past, including the creation of a do-not-call registry and a joint policy statement and public forum about the advertising of long distance services. *See* News Release, FCC, *Federal Trade Commission and Federal Communications Commission to Hold Joint Public Form on Advertising of Long Distance Services* (Sept. 23, 1999), *available at* http://ftp.fcc.gov/Bureaus/Common_Carrier /News_Releases/1999/nrcc9070.html; News Release, FCC, *Federal Communications Commission and Federal Trade Commission Issue Joint*

coalitions have worked together in the past to successfully attack similar problems, such as telephone fraud.[8] By acting aggressively to investigate and prosecute those parties that use illegal methods to obtain CPNI without customer consent, the Commission and FTC can eliminate any economic incentives for bad actors to buy and sell such data.

Given the threat posed by data brokers, Verizon supports the formation of a working group to gather intelligence and share tactics for combating unauthorized account access. Data brokers are often resourceful and could modify their methods for circumventing safeguards and obtaining protected information. In the *Notice*, the Commission recognized that this issue might best be addressed by an ongoing working group. *Notice* ¶ 25. Such a group would allow the industry to review how data brokers are obtaining CPNI and provide a shared resource for developing, modifying, and updating defensive security procedures. Verizon welcomes the opportunity to participate in a working group dedicated to protecting the privacy of our customers and combating unlawful access to customer accounts.

B. Customers Should Be Allowed, But Not Required, To Select A Password To Protect Their CPNI.

Verizon endorses the voluntary use of residential customer-set passwords as a CPNI safeguard; however, passwords should be available upon customer request, not as a mandate for all customers. *See Notice* ¶¶ 15-16. Verizon currently offers customers the ability to establish a personally selected password to protect their CPNI[9] and would support making the practice one

---

Policy Statement on Deceptive Advertising of Long Distance Telephone Services (Mar. 1, 2000), *available at* http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/2000/nrmc0009.html.

[8] *See* FCC Consumer Facts, *available at* http://www.fcc.gov/cgb/consumerfacts/businesstfrd.html (recommending customers contact the Alliance to Outfox Phone Fraud, "a broad-based group of telecommunications industry and related companies, serv[ing] to create public awareness about telephone fraud").

[9] Verizon requires customers establishing on-line accounts with Verizon.com to create a password.

of the criteria for qualifying for "safe harbor" protection. However, passwords are not an appropriate security solution for all customers in all circumstances. Indeed, according to a recent survey, 87 percent of customers asked about proposed legislation that would require some companies to mandate password protection were opposed to the idea of mandatory passwords.[10] Customers prefer having a choice of verifying their identity through passwords or through other objective identifiable personal data.[11] As explained below, in some cases, requiring a password may unnecessarily impede service or block legitimate transactions, or decrease the security of customer data. Moreover, imposing a new password requirement on an embedded base of customers would be costly for carriers and frustrating for consumers without yielding clear security benefits.

In the estimation of many consumers, the added security benefit of a customer-set password comes at too great a cost in terms of lost efficiency and convenience in conducting legitimate account transactions. Verizon agrees with EPIC and the Commission that the use of easily accessible biographical identifiers as a means of confirming customers' identity may be problematic if data brokers are able to obtain such information from publicly available records and pose as customers. *Notice* ¶ 15; EPIC Pet. at 8, 11. But customer-set passwords carry their own set of trade-offs. As an initial matter, many customers regularly forget or misplace passwords; surveys have reported that more than 80 percent of people have forgotten their passwords.[12] Where a password is lost or forgotten, a customer must go through the process of

---

[10] *See* Larry Ponemon, "Perceptions About Passwords," BNA Privacy and Security Law Report (Mar. 6, 2006).

[11] *Id.* (69% of customers prefer the option of having company provide "a *choice* of password or the use of three pieces of personal data to verify identity," rather than requiring one or the other (data identification or password) be used by all customers (emphasis added).

[12] *See id.* (88% of people surveyed had forgotten their password at least once in the past two years; 67% forgot their passwords three or more times in the past two years); *see also* Jason

resetting it. Some reports estimate that between 10 and 30 percent of help desk calls are for requests to reset passwords.[13] The business costs of addressing these password change requests can be significant.[14] Moreover, the cost to the customer of resetting passwords – a process that increases the time required to conduct routine transactions and requires customer authentication through the same sorts of inquiries passwords are intended to replace – is not simply monetary. A customer making only occasional account inquiries who is compelled to re-set a password multiple times will be deterred from obtaining information about his or her own account. If the password is required before obtaining information from a customer service representative over the telephone, a mandatory password requirement will inevitably lead to increased call handling

---

Hong et al., Attitudes and Behavior Towards Password Use on the Worldwide Web (Oct. 11, 2000) (almost 82% of people had forgotten a password established on a website), *available at* http://www.passwordresearch.com/stats/study48.html. For a link to various studies regarding passwords, *see* www.passwordresearch.com.

[13] *See* Axios Systems, Axios Systems Passwords Survey (Jan. 2003), *available at* http://www.passwordresearch.com/ stats/study68.html (more than one third of the survey's respondents said that password problems represented between 40 and 60 percent of all help desk calls; another 22.5 percent said password issues accounted for between 20 and 40 percent of calls; 6.5 percent putting the figure at between 60 and 80 percent); The Cost of Forgotten Passwords (Mar. 25, 2004), *available at* http://www.passwordresearch.com/stats/statistic162.html (Cox Communications estimated that 20% of help desk calls were to reset passwords); Help Desk Institute 2004 Practices Survey (Nov. 2004), *available at* http://www.passwordresearch.com/stats/statistic210.html (more than 17% of help desk calls were for password resets – more than calls for desktop operating system or software support); Password Management, Single Sign-On, and Authentication Management Infrastructure Products: Perspective (Jan. 7, 2002), *available at* http://www.passwordresearch.com/ stats/statistic167.html (password requests account for 25% of help desk calls); Gartner Group, Password Reset: Self-Service That You Will Love (Apr. 15, 2002), *available at* http://www.passwordresearch.com/ stats/study76.html (10% to 30% of help desk calls relate to password reset requests).

[14] Passwords Are Gobbling Up Your Profits (May 1, 2003), *available at* http://www.passwordresearch. com/stats/statistic94.html (2003) (reporting that it costs between $100 to $350 per user per year to manage passwords); Password Reset: Self-Service That You Will Love, *supra* (reporting password reset requests costs between $51 to $147 in labor costs); Citrix MetaFrame Password Manager (Sept. 2003), *available at* http://www.passwordresearch.com/stats/statistic95.html (password management costs estimated at $250 per user per year).

time. This is a source of frustration not only for the customer who may have trouble remembering a password but to all other customers in the queue.

In addition, requiring customer-set passwords could decrease the security of customer data. Confounded by password proliferation, many consumers afforded the option of establishing their own password re-use codes established for other purposes such as e-mail, credit card, or automatic teller machine access. And a large number of people admit to having shared their passwords with others.[15] Surveys also report that many users' passwords can be obtained simply by offering minimal inducements or using basic social engineering questions.[16] In the case of domestic disputes – which anecdotally appears to be a common source of CPNI data broker problems – a disgruntled spouse or partner may have access to the customer's password and other identifying information.[17] It may be appropriate for the FCC to remind spouses or partners in domestic dispute situations regarding the need to establish new passwords.

---

15 *See, e.g.*, Infosecurity Europe 2003 Information Security Survey (Apr. 2003), *available at* http://www.passwordresearch.com/stats/study55.html (two-thirds of workers surveyed had given their passwords to another colleague, and almost three quarters knew the passwords of another coworker).

16 *See, e.g., id.* (people surveyed used common words or readily obtainable biographical data (such as birthdates or family names), and ninety percent of those surveyed gave away their computer password for a cheap pen); Infosecurity Europe 2004 Information Security Survey (Apr. 2004), *available at* http://www.passwordresearch.com/ stats/statistic120.html (more than 70% of office workers surveyed "were willing to part with their password for a chocolate bar"; almost half of those surveyed said they would give their password to someone calling from the IT department, which left them "vulnerable to social engineering techniques," as hackers often pretend to call from the IT department and request a user's log on and password to "resolve a network problem").

17 Testimony of Steve Largent, President and Chief Executive Officer, CTIA-The Wireless Association, Before the U.S. House of Representatives Committee on Energy and Commerce, at 3 (Feb. 1, 2006) ("We've had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full social security number. Because many of these cases seem to arise in divorce or domestic cases, it is common for a spouse to have all of the necessary identifying information long after a divorce or separation to obtain call records.") ("CTIA House Testimony"), attached to Letter from Paul Garnett, CTIA, to Marlene H. Dortch, FCC, CC Docket No. 96-115, RM-11277 (filed Feb. 2, 2006).

Moreover, if the Commission were to require carriers to provide passwords to their entire embedded base of residential customers, the costs would be substantial, likely many tens of millions of dollars. In the face of an across-the-board password requirement, Verizon would need to contact millions of customers in a verifiable manner to obtain the requisite password. As the Commission recently experienced in overseeing efforts of VoIP providers to contact a relatively small number of customers about 911 availability – a life and death matter – even extraordinary outreach measures undertaken at great expense may fail to reach many consumers. As a result, for the majority of customers the process of establishing a password would not be initiated until the customer needed access to his or her CPNI. At that time, the need to authenticate the customer and establish a password would complicate, and possibly deter, a legitimate transaction.

In sum, although carefully selected and properly maintained passwords may offer additional privacy protection for some users, a rule requiring that all customer accounts be protected by customer-set passwords would not be a panacea. Nor would it necessarily lead to greater security than existing procedures that use carrier-established account verifiers such as customer account numbers or information from a recent bill. In contrast to a password requirement, making the practice of allowing residential customers to voluntarily select a password one of the criteria to qualify for "safe harbor" protection would be far less burdensome on residential consumers and carriers.

C. The Commission Should Support Carrier Efforts to Make Reasonable Revisions To Their Annual CPNI Filings.

The Commission should support carrier efforts to improve their annual CPNI filings by making reasonable revisions to the filings one of the criteria to qualify for "safe harbor" protection. As the Commission indicates in the *Notice*, carriers currently are required to sign a

compliance certificate on an annual basis verifying that the carrier has implemented procedures to adequately ensure compliance with the Commission's CPNI rules. *Notice* ¶ 29. Verizon supports the tentative conclusion that these certifications be filed with the Commission. *See id.* In addition, Verizon supports a rule requiring greater uniformity in dates for these certifications. But the date for the certifications should not be set at January 1. *Id.* Rather, if a carrier is certifying to the previous calendar year's CPNI practices, the deadline for certification should be one that gives the company adequate time to gather and review the necessary records from the prior calendar year. An appropriate deadline is April 1 or later.

In addition, the *Notice* proposes requiring carriers to include in their certifications (1) an explanation of any actions taken against data brokers and (2) a summary of consumer complaints regarding the unauthorized release of CPNI. *Id.* Verizon supports inclusion of the practice of making these additional disclosures among the criteria which will enable a carrier to qualify for "safe harbor" protection, so long as the disclosures are narrowly targeted to the potential data broker problem and are not over-inclusive. For example, carriers should *not* be required to report complaints that they investigated and determined to be without merit. In addition, the Commission should be aware that a summary of complaints may give other pretexters a roadmap on how to penetrate carrier security practices or could itself reveal confidential customer information. Thus, carriers must be allowed to summarize complaints of unauthorized access in the aggregate and/or have an option for requesting that the Commission grant confidential treatment of the summary.

D. The Commission Should Encourage The Practice Of Carriers Posting Their Privacy Policies Online, Enabling Customers To Evaluate Competing Privacy Protection Offers When Selecting A Carrier.

The Commission should encourage the practice of carriers posting their privacy policies online by making the practice one of the criteria to qualify for "safe harbor" protection. Because

most carriers already publish privacy policies on their websites, such a practice should not impose an unreasonable burden.[18] Making privacy policies publicly available and easily accessible will inform customers of the ways in which their data is being protected. In the highly competitive telecommunications marketplace, competitive market conditions and customer expectations will provide carriers with every incentive to protect customer privacy. Moreover, once properly informed, customers who are not satisfied with their carrier's privacy policies will be able to choose another carrier whose policies are more in line with their expectations.

E. The Commission Should Support The Carrier Practice Of Never Disclosing Certain Categories Of Information, Such As Social Security Number, Driver's License Number, And Taxpayer Identification Number, To The Customer.

The Commission should support the practice of carriers never releasing certain specified information to customers, such as social security number, driver's license number, or taxpayer identification number, by making the practice one of the criteria to qualify for "safe harbor" protection. Such a practice, however, should not prevent carriers from responding to calls from customers who want to confirm that the carrier has the correct information on file. For example, a customer that has a question about his or her credit rating and wants to ensure that the carrier has the correct social security number should be able to call a carrier and say, "I want to confirm that the social security number you have for me is xxx-xx-xxxx." A customer would be understandably frustrated if the carrier were forced to respond that it could neither confirm nor

---

[18] *See, e.g.*, Verizon, *Privacy and Customer Security Policies* (Jan. 2005), *available at* http://www22.verizon.com/about/privacy/customer/; Verizon Wireless Privacy Statement, *available at* http://www.verizonwireless.com/b2c/footer/privacy.jsp; Qwest, *Online Privacy Policy* (Sept. 29, 2005), *available at* http://www.qwest.com/legal/privacy.html; Sprint Nextel, *Sprint Privacy Policy* (Sept. 1, 2005), *available at* http://www.sprint.com/legal/sprint_privacy.html#principles; *see also* SBC, *Online Privacy Policy* (Sept. 19, 2005), *available at* http://www.sbc.com/gen/privacy-policy?pid=2506.

deny that the social security number the customer was providing was the same as the one used for a credit check.[19]

F. The Commission Should Establish An Enforcement "Safe Harbor" For Carriers That Have Implemented Reasonable CPNI Protections.

Given the evolving threat posed by data brokers, the Commission should establish an enforcement safe harbor for carriers acting reasonably to protect customer data. *See Notice* ¶ 26. As in other areas where fraud occurs, pretexters are resourceful and modify their methods for obtaining information. In this environment, though carriers may rigorously adhere to strict CPNI protection standards, some instances of unauthorized CPNI disclosure may still occur. The situation is akin to compliance with the agency's do-not-call rules, where some baseline of unauthorized contacts may occur even where carriers diligently work to reduce the likelihood of such occurrences and comply with the Commission's do not call rules. In the do-not-call context, the Commission found that treating each unauthorized contact as a *per se* violation was inappropriate and adopted an enforcement safe harbor.[20] The Commission should adopt a safe

---

[19] The Commission also should allow carriers the flexibility to release such information to others when necessary for legitimate business purpose. For example, when conducting a credit check on a customer, a social security number is routinely requested by consumer reporting agencies. *See, e.g.*, Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain, Before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly (Sept. 15, 2005) (statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues, U.S. Government Accountability Office), *available at* http://www.gao.gov/new.items/d051016t.pdf (reporting that credit reporting agencies regularly obtain and use social security numbers).

[20] Under the do-not-call safe harbor, a carrier is not subject to enforcement, even if an unauthorized contact occurs, provided that: (1) it has established and implemented written procedures to comply with the national do-not-call rules; (2) it has trained its personnel and any entity assisting in its compliance in procedures established pursuant to the national do-not-call rules; (3) it has maintained and recorded a list of telephone numbers that the seller may not contact; (4) it uses a process to prevent telephone solicitations to any number on any list established pursuant to the do-not-call rules; and (5) it uses a process to ensure that it does not sell, rent, lease, purchase or use the national do-not-call database for any unlawful purpose. 47 C.F.R. § 64.1200(c)(2).

harbor here as well, protecting carriers that have adopted reasonable safeguards to protect against unauthorized disclosures in good faith compliance with Commission requirements. Carriers that have adopted reasonable practices for protecting customer privacy – such as (1) cooperating with FCC, FTC, and DOJ efforts to identify and prosecute data brokers, (2) participating in a carrier working group dedicated to enhancing data security and combating theft of confidential information; (3) permitting customers, on a voluntary basis, to elect password protection for residential accounts; (4) filing more detailed annual CPNI certifications with the FCC; (5) posting privacy policies online; and (6) establishing certain categories of information, such as social security, driver's license, and taxpayer identification numbers, that should not be disclosed to residential customers – should not be punished by enforcement action and monetary forfeitures for the wrongful actions of third party data brokers that may occasionally be able to circumvent even well-designed CPNI protections.

II. THE COMMISSION SHOULD REJECT EXPENSIVE, BURDENSOME MEASURES WITH LITTLE OR NO DATA SECURITY BENEFIT.

Verizon shares the Commission's and EPIC's concern regarding unauthorized disclosure of CPNI and interest in developing effective safeguards for preventing incursions by data brokers. *See generally Notice*; EPIC Pet. But no safeguard, or mix of safeguards, is infallible in the face of a dynamic, ever-changing threat. Accordingly, no single approach should be frozen in place through regulation. The Commission should ensure that carriers retain the flexibility needed to address evolving data broker tactics while still providing high quality service to customers. Moreover, while security is an important goal, it must be balanced against other concerns. The requirements proposed by EPIC, if mandated for all carriers, systems, and customer data, would impose significant burdens and costs – both to carriers and their customers – that far outweigh the potential benefits in terms of addressing inappropriate data broker

practices.

A. The Commission Has Already Rejected A Requirement To Keep An Audit Trail Of All CPNI Disclosures As Overly Burdensome And Unnecessary.

The Commission should not adopt stringent audit trail requirements in this proceeding for the same reason the Commission has rejected them in the past: such requirements are inordinately expensive and are not closely targeted to protecting CPNI. *See Notice* ¶¶ 17-18. Verizon currently trains its representatives to make entries in the account record for certain CPNI transactions, including a notation on the customer's account of when he or she has called customer service requesting specific information. Other carriers report similar practices. *See id.* ¶¶ 17-18 & n.49. The Commission, however, has properly rejected more stringent audit trail requirements – such as EPIC's suggestion to "require carriers to record *all* instances when a customer's records have been accessed, whether information was disclosed, and to whom" – as an inordinately expensive measure, with costs that far outweigh the potential benefits. *Id.* ¶ 17 (emphasis added).

The Commission previously adopted an audit trail requirement but quickly reversed itself on reconsideration when the industry pointed out the enormous costs to modify systems to meet the requirements and to maintain the necessary databases to track this information.[21] Indeed, the Commission cited an estimate from one carrier that it alone would have to spend more than $270 million to comply with the new rule. *Second Report and Order* ¶ 124. A number of other commenters warned that the audit trail requirement would be "particularly burdensome for small

---

[21] In the *Second Report and Order* the Commission mandated audit trails in order to encourage carrier compliance and to create a method of verification where disputes arose. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) ("*Second Report and Order*").

and rural carriers." *Id.* ¶ 125. On reconsideration, the Commission recognized that the audit trail requirement was "a potentially costly and burdensome rule [that] does not justify its benefit."[22] The *Reconsideration Order* acknowledged that existing rules already required carriers to protect CPNI and that carriers had existing internal procedures to do so. The same is true today. And seven years later, carriers are further invested in carrier-specific audit procedures and the costs of changing course have only increased.

In addition, adopting audit trail requirements likely would provide only limited benefits in addressing the data broker problem. It appears that in most cases, data brokers obtain confidential customer data by pretending to be someone who can legitimately access customer data.[23] If that is the case, an audit trail may reveal only that someone purporting to be the customer called and asked about customer detail – something that would not be helpful in preventing data broker access to such records or tracking the wrongdoer to a specific person. Given these costs and the lack of tangible security benefits, the Commission should affirm its prior decision rejecting an audit trail requirement.

EPIC has noted in the past that carriers are required to maintain audit trails of the use of CPNI in specific marketing campaigns and suggested that audit trail requirements would be

---

22 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended,* Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 127 (1999) ("*Reconsideration Order*").

23 *See, e.g.*, Written Statement of Kris Anne Monteith, Chief, Enforcement Bureau, FCC, Before the Subcommittee on Consumer Affairs, Product Safety, and Insurance Committee on Commerce, Science and Transportation, United States Senate, on "Protecting Consumers' Phone Records," at 5 (Feb. 8, 2006) ("The carriers [that spoke with the FCC Enforcement Bureau staff] generally expressed their belief that the problems they have experienced in this area are largely, if not exclusively, related to attempts by individuals outside the company to obtain information through pretexting, rather than by 'rogue' employees selling information to data brokers."); CTIA House Testimony, at 2 ("Overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of "pretexting," which is nothing more than lying to obtain something you aren't entitled to procure lawfully.").

workable to address the data broker problem as well. *See Notice* ¶ 17 & n.47. In the case of marketing campaigns, however, carriers need only track calls that are initiated by the carrier and that can be limited to a certain number of customers, which facilitates the tracking and control of specific call data. By contrast, the volume of potential data that would have to be tracked in order to conduct an audit trail for all CPNI is enormous. Verizon handles, on average, more than 400,000 residential customer calls per business *day*. As the Commission has previously concluded, the costs in money and time to obtain, record, and archive *detailed* information about each of these calls – including the specific customer data accessed or disclosed – are substantial. It would require re-engineering systems and company-wide re-training, an exceedingly costly and time-consuming proposition. It would also significantly increase the time for handling customer calls if a representative were required to record every customer record accessed whenever responding to a customer request for information.

B. Although Encryption May Have A Role In the Protection Of Confidential Data, It Is Not Well-Tailored To The Safeguarding Of CPNI.

While Verizon uses encryption as part of its data protection strategy, the company opposes a requirement to encrypt *all* customer records containing CPNI. Again, this would not be a cost-effective way to protect customer data because there is no evidence that data brokers access customer accounts via hacking. *See Notice* ¶ 19.

Verizon currently uses encryption in a variety of circumstances to protect confidential data.[24] For example, the company provides added protection to sensitive customer data by transmitting it through a secure connection.[25] Even for this purpose, however, encryption offers

---

[24] *See* Verizon, *Privacy and Customer Security Policies* (Jan. 2005), *available at* http://www22.verizon.com/about/privacy/customer/.

[25] *See* Verizon, *Internet Privacy Policy*, *available at* http://www22.verizon.com/privacy/index/#secure ("Verizon uses Secure Socket Layer (SSL) to transmit sensitive information such as credit card numbers and SSN. SSL is a transport level technology for authentication and data

no guarantee of security. Encryption chiefly deters smaller hackers with fewer resources while better financed wrongdoers with more advanced equipment may still penetrate databases secured even with sophisticated encryption – a problem not unique to telecommunications but faced by every industry that handles electronically-stored sensitive data.

Moreover, there is no evidence to suggest that the unauthorized release of customer data is caused by data brokers hacking into carriers' systems. Again, it appears that data brokers proceed by deceit and impersonation through pretexting or social engineering, fraudulently convincing customer service personnel that they have authorized access to an account. Encryption of data within a carrier's internal database is no protection when a customer service representative believes he or she is speaking with an authorized account holder and will therefore release CPNI whether it is encrypted or not. A requirement to encrypt records would impose significant costs that cannot be justified,[26] particularly in the absence of any demonstrated benefit in deterring data brokers or enhancing security beyond its current level.

C. Carriers Require Flexibility In Their Data Retention Practices To Meet A Variety of Objectives And Legal Requirements, Including Protection of CPNI.

The Commission should not require carriers to delete call records when they are no longer necessary for billing or dispute purposes or, alternatively, require that carriers "de-

---

encryption between a Web server and a Web browser. SSL sends data over the "socket" which is a secure channel at the connection layer.").

[26] The cost of encrypting all CPNI located in all of Verizon's systems would likely be many tens of millions of dollars, presuming "encryption" means the Advanced Encryption Standard ("AES") adopted by the National Institute of Standards and Technology. Adoption of a rule requiring all CPNI to be encrypted would require Verizon to upgrade all of its databases to the current versions, reload the data, update all applications accessing the data, and double its available storage for encrypted CPNI. As part of this process, Verizon must deeply examine *all* of its applications. Many applications access data in a database and then "cache" it in ad hoc structures outside of the database for faster manipulation. In order to ensure that all data is encrypted, Verizon would have to identify all of these ad hoc uses of data and encrypt each one. This entire process would likely take between two and three years.

identify" records, *i.e.*, "separate data that identify a particular caller from the general transaction records." EPIC Pet. at 11; *Notice* ¶ 20. This suggestion fails to recognize that carriers retain customer records containing CPNI for a variety of reasons unrelated to billing and disputes. Such records are frequently needed and retained in the usual course of business for use in civil and criminal litigation. They also are regularly used to respond directly to customer inquiries[27] and for fraud detection and follow-up investigations. Even the FCC's rules contain data retention requirements that may be at odds with EPIC's proposal. For example, EPIC's deletion plan, which imposes a strict deletion rule when data is no longer needed for billing purposes or disputes, may be contrary to the Commission's Part 42 rules requiring that carriers retain telephone toll records for 18 months[28] and all other records for the period established in the carrier's data retention index.[29] Even after the customer has left the company, there may be a number of reasons why a carrier may lawfully access the customer's information, such as to respond to law enforcement requests, to engage in "winback" campaigns, or to address potential allegations of slamming.[30] Moreover, there is no evidence that older records are more susceptible to fraudulent disclosure than newer ones.[31] Therefore, there is no reason to require

---

27 Customers often request this information to determine whether they are on the appropriate plan, divide up monthly charges in a roommate situation, and a variety of other reasons.

28 47 C.F.R. § 42.6.

29 47 C.F.R. § 42.7.

30 *See Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶¶ 66-74 (1999) (eliminating the rule prohibiting the use of CPNI in winback campaigns); 47 C.F.R. § 64.1100 *et seq.* (subjecting telecommunications carriers to obligations regarding subscribers' change of telecommunications provider).

31 *See* CTIA Comments, RM-11277, at 19-20 (filed Oct. 31, 2005).

carriers to delete customer records containing CPNI prior to the date specified under the company's existing document deletion schedule or when the statute of limitations has run on any potential dispute.[32]

D. The Commission Should Reject Customer Notification Rules As Unwieldy And Potentially Detrimental To Data Security.

A requirement to notify customers of unauthorized release of CPNI is not a viable solution to data broker incursions and would produce unnecessary customer concern and confusion that far outweigh any potential security benefit. *Notice* ¶¶ 21-24. As an initial matter, a customer notification requirement is not closely targeted to addressing the data broker problem. Because anecdotal reports indicate that most data brokers operate via pretexting, a significant problem with any notification requirement is that a carrier is not likely to know when any breach of security protections has occurred.

Notification in the case of unconfirmed breaches is particularly problematic. By referring to situations in which security "may" have been breached, the *Notice* suggests that the Commission might require carriers to notify customers of possible, unconfirmed breaches of CPNI.[33] Requiring notification too early could result in carriers "notifying" customers of problems that do not actually exist. This might lead to a flurry of notices, which would result in customers being desensitized to cases where an actual privacy breach occurs and undermine customers' confidence in their carriers' ability to protect their confidential data.

---

[32] As with required encryption, the costs of de-identifying CPNI would likely be many tens of millions of dollars. Although de-identification implies less specific standards than encryption, the costs associated with de-identification are largely the same as those for encryption because logical and physical modifications to the database schema are required.

[33] *See Notice* ¶ 21 ("EPIC suggests that companies notify customers when the security of their CPNI *may* have been breached." (emphasis added)).

Relatedly, the *Notice* asks about "the costs and benefits of routinely notifying customers after any release of their CPNI, including incidents where the carrier has no grounds to suspect that the request is not legitimate. For example, should carriers include a statement on or with the customer's invoice for every occurrence when that customer's CPNI records have been accessed?" *Notice* ¶ 23. Again, the answer to that question is "no." As an initial matter, although the concept of notice sounds simple, for most carriers, in reality it would require significant systems work. The notice itself would be expensive because it would require reworking of a carrier's existing bill structure to put a notice on customer bills, or a separate customer mailing every time a customer calls to ask about his or her account. Costs likely would not be limited to the notice itself, however. A rule requiring customer notice almost certainly would lead to an increase in customer calls asking for information about how and when their account information was accessed. In order to provide customer service representatives with information to respond to these calls, carriers may essentially be forced to create the same type of audit trail systems that the Commission has already declined to require. *See* Section II.A. This could also dramatically increase the costs associated with customer service representative responses to customer calls, and, if there is a significant increase in call volume, may lead to a general increase in the average call handling time, which will lead to customer irritation as well. In total, these costs are likely to be tens of millions of dollars.

The *Notice* also asks commenters about "the potential value of notification as a precautionary measure *before* releasing CPNI." *Notice* ¶ 22 (emphasis added). As a practical matter, prophylactic customer notification before releasing CPNI is unwieldy. In order to comply with such a requirement, carriers would be required to contact a customer at an address or phone number of record, typically a home address or phone number, before disclosing CPNI.

Customer inquiries, however, typically occur during regular business hours when the customer is away from home, making it impossible to verify a customer's CPNI request in real time or even in a single transaction. In Verizon's experience, customers already are frustrated by the amount of time it takes for customer authentication. Requiring precautionary customer notification would only compound this frustration and deter or slow legitimate transactions. Moreover, like notices of unconfirmed security breaches, requiring repeated notices may diminish customer data security by allowing notices of suspected unauthorized disclosure to get "lost in the shuffle."

E. The Commission Should Reject The Proposal Permitting Customers To Put An Absolute "No Release" Order On Their CPNI As Inconsistent with Section 222.

The Notice asks whether carriers should be required "to permit customers to put an absolute 'no release' order on their CPNI, possibly subject to existing exceptions in section 222(c)(1)?" *Notice* ¶ 24. It should not. A "no release" order for all CPNI would be overbroad, and, if it did not allow for disclosures authorized under the exceptions to Section 222, would violate the statute.[34]

As an initial matter, the Commission does not have the authority to impose rules that would restrict carriers from releasing CPNI in instances where the statute specifically allows carriers to do so without customer consent. *See* 47 U.S.C. § 222. Among other things, the statute specifically allows carriers to use CPNI *without* customer consent for billing and collection purposes, to protect against fraud, to provide inbound telemarketing or other services to a customer who initiates a call, and as otherwise "required by law." *Id.* § 222(c)(1), (d). Thus, customers who believe that they are making a categorical ban on release of CPNI will be

[34] The Commission should adopt a rule providing that carriers will not release certain specified information to customers, such as social security number, drivers' license identification number, or taxpayer identification number. *See* Section I.E., above.

confused and frustrated to learn that there are a number of situations in which their CPNI can still be shared.[35] Moreover, the *Notice* does not propose what would occur if a customer makes a "no release" election and then changes his mind and does want access to his own CPNI. If the carrier insists that the "no release" election is permanent and cannot be changed, the customer will be understandably frustrated. If there are situations in which the Commission will allow carriers to change the "no release" option – such as if the customer can verify by password or other objective information that he authorized to make the change – the "no release" election is no more stringent a control than simply requiring such information (such as password or other objective information) be made available before CPNI is released.

F. Any New Measures Designed To Protect Residential Customer Data Should Not Be Extended To Business Customers.

The Commission's policies should allow carriers and their customers the ability to tailor privacy solutions to best meet customers' needs. In particular, the Commission's rules should recognize that the data broker problem is targeted primarily at residential customer data. Many business customers have their own security solutions and will not need additional security protections tailored for the data broker problem affecting residential customers. Business customers often have a greater need for efficiency and convenience in receiving information about their accounts because their bills tend to be larger and may require more detailed review than residential customer accounts.

Thus, proposals that may be appropriate for protecting the information of residential customers would not be appropriate or necessary for business customer accounts. For example,

---

[35] For example, if a customer under a "no release" order were to call and ask whether he or she might save money under another service plan or bundled offering, the "no release" order would prevent a customer service representative from answering the question. The representative would not be authorized to retrieve the customer's records to compare his or her existing to plan to other available service offerings.

the *Notice* asks how CPNI is provided to customers (via telephone, regular mail, e-mail, or fax) and whether there should be any limitations on the transmission of CPNI. *Notice* ¶ 13. A rule prohibiting the faxing of account information to a residential customer might impose minimal burdens and inconvenience and be in keeping with customer privacy expectations; however, business customers typically have different needs to obtain information quickly and may place a premium on efficiency. Given that data brokers are targeting residential customers and business customers often have different or specialized security needs, the Commission should not impose any new CPNI rules for services provided to business customers.

III. THE COMMISSION SHOULD REJECT CALLS TO REVISIT SETTLED LAW WITH RESPECT TO OPT-IN/OPT-OUT CONSENT.

There is no need for the Commission to reconsider opt-out authorization for sharing CPNI with joint venture partners and independent contractors, and doing so raises legal risks and policy concerns. *See Notice* ¶ 12. As an initial matter, there is no evidence in the *Notice* or elsewhere for the proposition that joint venture partners and independent contractors are the source of CPNI leaks exploited by data brokers. Moreover, changing the opt-out rules to more stringent regulation likely would face significant constitutional legal challenges and would impede the flow of useful information desired by customers.

The Commission's opt-out rules do not have any connection to the data broker problem. The opt-out mechanism allows carriers to infer that their customers have consented to sharing CPNI with the carrier's affiliates, third party contractors, agents, and joint venture partners that provide communications-related services, unless a customer specifically states he or she does not want his or her information shared (*i.e.*, "opts out"). Under the opt-out rules, companies may only share information under strict confidentiality conditions and only with entities that have a direct relationship to the carrier. *See Notice* ¶ 12 & n.35; 47 C.F.R. § 64.2007(b)(2). There is no

evidence that data brokers are obtaining information from independent contractors or joint venture partners. Thus, changing the opt-out rules is likely to have no impact on data broker access to customer data.

In addition, the opt-in requirements proposed in the *Notice* have no prospect of surviving First Amendment scrutiny. In striking down a Commission rule requiring carriers to obtain customer opt-in approval prior to using CPNI to market out-of-bucket services on First Amendment grounds, the Tenth Circuit concluded that the FCC failed to carry its burden of demonstrating both that the regulation materially advanced the interest claimed and was narrowly tailored.[36] The Court determined that the FCC did not base its regulation on any evidence of real harm to consumers arising from the use of CPNI the regulation would have had the effect of limiting.[37] Moreover, with respect to the breadth of the impact of an opt-in approach on protected speech, the Court stated: "[T]he FCC's failure to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor the CPNI regulations regarding customer approval."[38]

On remand, the Commission adopted the opt-out rule that applies today after concluding that, despite extensive fact gathering and record development, it could not articulate a constitutional basis for requiring opt-in. In the wake of the Tenth Circuit's ruling, the FCC conducted an exhaustive proceeding to examine whether *any* empirical evidence existed to support an opt-in regime. It found that no such evidence existed and concluded that an opt-in regime was overly restrictive of carrier speech and could not survive First Amendment

---

36 *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

37 *Id.* at 1237.

38 *Id.* at 1238.

scrutiny.[39] Accordingly the Commission adopted an opt-out approach allowing carriers to use CPNI to market out-of-bucket services and to share CPNI with joint venture partners and independent contractors – the approach codified in Section 64.2007(b) of the Commission's current rules. 47 C.F.R. § 64.2007(b).

At the state-level, public utility commission rules requiring opt-in authorization have met the same fate as federal rules. In November 2002, after the FCC's *Third CPNI Order*, the Washington Utilities and Transportation Commission adopted CPNI rules containing an opt-in requirement.[40] Verizon challenged the rules on the grounds that they restricted carriers' and customers' free speech rights in contravention of the First Amendment and were preempted by federal law. The Federal District Court for the Western District of Washington agreed, striking down the Washington rules on First Amendment grounds and granting Verizon summary judgment.[41]

Nothing has changed since the 10th Circuit and Western District of Washington decisions to improve the constitutional standing of an opt-in approach. Because the "less restrictive alternative" embodied in current FCC rules – an opt-out approach – is adequate to address customers' privacy interests, the Commission could not demonstrate that the stringent opt-in requirement proposed in the *Notice* is sufficiently narrowly tailored to withstand constitutional

---

39 *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, Third Report and Order and Third Notice of Proposed Rulemaking, CC Docket No. 96-115, FCC 02-214 (rel. July 25, 2002) (1998) ("*Third CPNI Order*"), Statement of Chairman Michael K. Powell ¶ 1.

40 *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1188-89 (W.D. Wash. 2003).

41 *Id.* at 1187.

scrutiny.[42] As an initial matter, where the purported objective in adopting an opt-in is combating the data broker threat, the proposed regulation does not advance the identified governmental interest. There is no evidence data brokers have targeted carriers' independent contractors and joint venture partners in their efforts to gain unauthorized access to customer data. Moreover, Congress has determined that a notice and opt-out regime adequately protects consumers' privacy interest in other situations, including those involving far more sensitive, private information.[43] Thus, while both opt-in and opt-out can effectively advance the governmental interest in protecting customer privacy, opt-in deprives a substantial number of consumers of commercial information they desire to receive.[44] Given that opt-out is an effective alternative, it is inconceivable that any new opt-in requirement could be shown to be "'no more extensive than necessary'" to protect the government's interest.[45]

---

42 *See, e.g., U.S. West*, 182 F.3d at 1238.

43 Under the 1996 Consumer Credit Reporting Reform Act, for example, credit reporting agencies may furnish consumer credit information for marketing credit or insurance opportunities to consumers, so long as the agency establishes a toll-free number so that consumers can call and opt-out by having their names removed from lists for direct marketing purposes. 15 U.S.C. § 1681b(e)(5).

44 *Third CPNI Order* ¶¶ 36, 71. In addition, consumers understand and utilize the opt-out procedures when they desire to protect their privacy. *See* Public Attitudes Toward Local Telephone Company Use of CPNI: Report of a National Opinion Survey Conducted November 14-17, 1996 by Opinion Research Corporation, Questions 5, 6, 10-11, Analysis at 9-10, Princeton, N.J. and Prof. Alan F. Westin, Columbia University, Sponsored by Pacific Telesis Group (now SBC).

45 *U.S. West*, 182 F.3d at 1238 (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 486 (1995)). *See also 44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 507 (1996); *id.* at 529 (O'Connor, J., concurring) ("The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny."); *Bd. of Trustees of the State Univ. of N.Y. v. Fox*, 492 U.S. 469, 479 (1989) ("[A]lmost all of the restrictions disallowed under *Central Hudson*'s fourth prong have been substantially excessive, disregarding 'far less restrictive and more precise means.'" (citing *Shapero v. Ky. Bar Ass'n.*, 486 U.S. 466, 476 (1988); *Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio*, 471 U.S. 626 (1985); *In re R.M.J.*, 455 U.S. 191 (1982); *Bates v. State Bar of Ariz.*, 433 U.S. 350 (1977))).

Furthermore, requiring opt-in approval before carriers could share CPNI with independent contractors or joint venture partners would be inappropriate as a matter of policy. As the Commission has previously found, "[e]nabling carriers to communicate with customers in this way is conducive to the free flow of information, which can result in more efficient and better-tailored marketing and has the potential to reduce junk mail and other forms of unwanted advertising." *Third CPNI Order* ¶ 35. Thus, the Commission recognized that "consumers may profit from having more and better information provided to them, or by being introduced to products or services that interest them." *Id.* By contrast, adopting more stringent opt-in regulations for sharing such information with independent contractors or joint venture partners would simply increase the cost of targeted marketing campaigns. Adopting opt-in restrictions on use of CPNI may lead to *more unwelcome* marketing to consumers because if carriers are not able to use CPNI, they may have to engage in broader, mass-market campaigns, based on demographic data supplied by third parties. If carriers cannot use CPNI to target offers for new products, services, and packages to those customers most likely to want them, this will lead to an increase in marketing to those consumers for whom the product or service is inappropriate or who are not interested in purchasing it.

IV. CONCLUSION

The Commission should encourage a number of practices that enhance protection of subscriber data by making them the basis for "safe harbor" protection from enforcement action. Specifically, Verizon supports a "safe harbor" incorporating the following practices: (1) cooperating with FCC, FTC, and DOJ efforts to identify and prosecute data brokers, (2) participating in a carrier working group dedicated to enhancing data security and combating theft of confidential information; (3) permitting customers to voluntarily elect password protection for residential accounts; (4) filing more detailed annual CPNI certifications with the FCC; (5)

posting privacy policies online; and (6) establishing certain categories of information – such as social security, driver's license, and taxpayer identification numbers – that should not be disclosed to residential customers. Carriers adopting these practices should receive "safe harbor" protection from enforcement action, consistent with the Commission's approach in the do-not-call context.

The Commission should reject other measures proposed in the *Notice* as unduly burdensome and adding little or no data security benefit. In particular, the agency should reject proposals to require: (1) audit trails; (2) encryption; (3) data retention or deletion requirements; (4) customer notification of CPNI disclosures; and (5) the option of an "absolute" no CPNI disclosure order for customer accounts. In all cases, the FCC should be careful to distinguish between the needs of residential and business customers and should not adopt any new measures for business customers. Finally, the Commission should reject calls to revisit settled law with respect to opt-in/opt-out consent.

Respectfully submitted,

By: Joshua Swift / by SDD

Karen Zacharia
Joshua E. Swift
VERIZON
1515 N. Court House Road
Suite 500
Arlington, VA 22201-2909
703.351.3039

Scott Delacourt
Wiley, Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006

Counsel for Verizon

Of Counsel
Michael E. Glover

Dated: April 28, 2006